PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

(Chapter II of the Patent Cooperation Treaty)

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference 15739PCT00	**FOR FURTHER ACTION**	See Form PCT/IPEA/416
International application No. PCT/DK2005/000090	International filing date *(day/month/year)* 10.02.2005	Priority date *(day/month/year)* 10.02.2004
International Patent Classification (IPC) or national classification and IPC INV. H04L9/32		
Applicant CRYPTICO A/S et al.		

1. This report is the international preliminary examination report, established by this International Preliminary Examining Authority under Article 35 and transmitted to the applicant according to Article 36.
2. This REPORT consists of a total of 8 sheets, including this cover sheet.
3. This report is also accompanied by ANNEXES, comprising:

   a. ☒ *sent to the applicant and to the International Bureau)* a total of 6 sheets, as follows:

   ☒ sheets of the description, claims and/or drawings which have been amended and are the basis of this report and/or sheets containing rectifications authorized by this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions).

   □ sheets which supersede earlier sheets, but which this Authority considers contain an amendment that goes beyond the disclosure in the international application as filed, as indicated in item 4 of Box No. I and the Supplemental Box.

   b. □ *(sent to the International Bureau only)* a total of (indicate type and number of electronic carrier(s)) , containing a sequence listing and/or tables related thereto, in electronic form only, as indicated in the Supplemental Box Relating to Sequence Listing (see Section 802 of the Administrative Instructions).

4. This report contains indications relating to the following items:

☒	Box No. I	Basis of the report
□	Box No. II	Priority
□	Box No. III	Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
☒	Box No. IV	Lack of unity of invention
☒	Box No. V	Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
□	Box No. VI	Certain documents cited
☒	Box No. VII	Certain defects in the international application
□	Box No. VIII	Certain observations on the international application

Date of submission of the demand 15.09.2005	Date of completion of this report 12.06.2006
Name and mailing address of the international preliminary examining authority: European Patent Office - P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk - Pays Bas Tel. +31 70 340 - 2040 Tx: 31 651 epo nl Fax: +31 70 340 - 3016	Authorized officer Holper, G Telephone No. +31 70 340-2304

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

International application No.
PCT/DK2005/000090

Box No. I Basis of the report

1. With regard to the **language**, this report is based on

   ☒ the international application in the language in which it was filed

   □ a translation of the international application into , which is the language of a translation furnished for the purposes of:
   - □ international search (under Rules 12.3(a) and 23.1(b))
   - □ publication of the international application (under Rule 12.4(a))
   - □ international preliminary examination (under Rules 55.2(a) and/or 55.3(a))

2. With regard to the **elements*** of the international application, this report is based on *(replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report)*:

Description, Pages

1-13	as originally filed

Claims, Numbers

1-47	received on 19.05.2006 with letter of 16.05.2006

Drawings, Sheets

1/5-5/5	as originally filed

□ a sequence listing and/or any related table(s) - see Supplemental Box Relating to Sequence Listing

3. □ The amendments have resulted in the cancellation of:
   - □ the description, pages
   - □ the claims, Nos.
   - □ the drawings, sheets/figs
   - □ the sequence listing *(specify)*:
   - □ any table(s) related to sequence listing *(specify)*:

4. □ This report has been established as if (some of) the amendments annexed to this report and listed below had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).
   - □ the description, pages
   - □ the claims, Nos.
   - □ the drawings, sheets/figs
   - □ the sequence listing *(specify)*:
   - □ any table(s) related to sequence listing *(specify)*:

* If item 4 applies, some or all of these sheets may be marked "superseded."

Box No. IV Lack of unity of invention

1. □ In response to the invitation to restrict or pay additional fees, the applicant has, within the applicable time limit:

   □ restricted the claims.

   □ paid additional fees.

   □ paid additional fees under protest and, where applicable, the protest fee.

   □ paid additional fees under protest but the applicable protest fee was not paid.

   □ neither restricted the claims nor paid additional fees.

2. ☒ This Authority found that the requirement of unity of invention is not complied with and chose, according to Rule 68.1, not to invite the applicant to restrict or pay additional fees.

3. This Authority considers that the requirement of unity of invention in accordance with Rules 13.1, 13.2 and 13.3 is:

   □ complied with.

   ☒ not complied with for the following reasons:

   see separate sheet

4. Consequently, this report has been established in respect of the following parts of the international application:

   ☒ all parts.

   □ the parts relating to claims Nos. .

Box No. V Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	1-47
	No:	Claims	
Inventive step (IS)	Yes:	Claims	1-47
	No:	Claims	
Industrial applicability (IA)	Yes:	Claims	1-47
	No:	Claims	

2. Citations and explanations (Rule 70.7):

   see separate sheet

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

International application No.
PCT/DK2005/000090

Box No. VII Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

see separate sheet

Re Item IV

This Authority considers that there are three inventions covered by the claims indicated as follows:

I: Claims 1-20 are directed to a method for generating an identification value for identifying an electronic massage in a MAC in which data representing the length L of the message are concatenated to the output or to an intermediate result.

II: Claims 21-40 are directed to a method for generating an identification value for identifying an electronic massage in a MAC in which an auxiliary hash function having a different compression rate is applied to an unprocessed data block if n does not divide the number m_i of input blocks.

III: Claims 41-47 directed to method for generating an identification value for identifying an electronic message using a delta-universal hash function and a sum of the resulting number and a further block of data.

The reasons for which the inventions are not so linked as to form a single general inventive concept, as required by Rule 13.1 PCT, are as follows:

Although the problems dealt with by the independent claims 1, 21 and 41 are linked or identical, the solutions defining the special technical features are not the same nor corresponding, contrary to Rule 13.2 PCT (see point V below).

Re Item V

Reasoned statement with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

Reference is made to the following document:

D1: MATSUO T ET AL: "ON PARALLEL HASH FUNCTIONS BASED ON BLOCK-CIPHERS" IEICE TRANSACTIONS ON FUNDAMENTALS OF ELECTRONICS, COMMUNICATIONS AND COMPUTER SCIENCES, INSTITUTE OF ELECTRONICS INFORMATION AND COMM. ENG. TOKYO, JP, vol. E87-A, no. 1, January 2004 (2004-01), pages 67-74, XP001185960 ISSN: 0916-8508

The application concerns three methods (claims 1, 21 and 41) for generating an identification value for identifying an electronic message, three computer systems (claims 19, 39, 46) programmed to carry out said methods as well as computer program products (claims 20, 40, 47) for performing said methods.

The document D1 is regarded as being the closest prior art to the subject-matter of claim 1 and shows (the references in parentheses applying to this document, see fig.3):
a method for generating an identification value based on parallel hash functions applied in a tree structure (three rounds) where a residual data block (m_5) is passed without compression from the current level to another subsequent level (3rd level) in case n does not divide the number m_i of input blocks for said current level.

The subject-matter of claim 1 differs from this known method in that data which represent the length L of the message are concatenated to the output or one of the intermediate results.

The subject-matter of claim 1 is therefore new (Article 33(2) PCT).

The problem to be solved by the present invention may be regarded as how to avoid an intentional modification of the input message length which could not be detected by the known method.

The solution to this problem proposed in claim 1 of the present application is considered as involving an inventive step (Article 33(3) PCT) for the following reasons:
Appending data representing the length L of the input message during consecutive hashing is not know nor suggested by the prior art.

Concerning method claim 21, the closest prior art is also illustrated by D1.
The problem to be solved by method claim 21 is to find an alternative solution for avoiding the padding of zero blocks in the Damgard construction and thus to reduce the total number of hash functions.
According to claim 21 this problem is solved by using an auxiliary hash function having a compression rate which is different from the compression rate of a first hash function.
Using different compression rates during the generation of a MAC is not known nor

suggested in the prior art.

Claims 2-18 are dependent on claim 1 and claims 22-38 are dependent on claim 21; as such they also meet the requirements of the PCT with respect to novelty and inventive step.
Concerning method claim 41 the closest prior art is again illustrated by D1.
The problem to be solved is again to find an alternative for reducing the number of hash functions used during compression as compared to the Damgard construction.

According to claim 41 this problem is solved by computing the sum of the result of a delta-hash function and a further block which is not hashed. This processing step is not known nor suggested by the prior art.

Claim 42-45 are dependent on claim 41 and as such also meet the requirements of the PCT with respect to novelty and inventive step.

Claims 19 and 20, 39 and 40, 46 and 47 define computer systems and computer program products carrying out the methods of claims 1, 21 and 41 respectively. As such they also meet the requirements of the PCT with respect to novelty and inventive step.

Re Item VII

Independent claim 1 is not in the correct two-part form in accordance with Rule 6.3(b) PCT, which in the present case is appropriate, with those features known in combination from the prior art (document D1) being placed in the preamble (Rule 6.3(b)(I) PCT) and with the remaining features being included in the characterising part (Rule 6.3(b)(ii) PCT).

In the present case, the following features are known in combination from the document D1 and belong in the preamble of such a claim:
a residual data block is passed without compression from the current level to another subsequent level in case n does not divide the number of input blocks m_i for said current level.

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY (SEPARATE SHEET)

International application No.

PCT/DK2005/000090

The features of the independent method claims are not provided with reference signs placed in parentheses (Rule 6.2(b) PCT).

PCT application No. PCT/DK2005/000090
Owner: Cryptico A/S
Title: Methods for Generating Identification Values for Identifying Electronic Messages
Our ref: 15739PCT00

New claims under Art. 34 PCT
16 May 2006

CLAIMS

1. A method for generating an identification value for identifying an electronic message in a Message Authentication Code (MAC) function by application of at least one first hash function with fixed compression that compresses n blocks of data into a number of blocks which is smaller than n or into one single block, the hash function being repetitively applied in a tree-structure compression of the message, so that the message is being compressed in a plurality of tree-structure levels, each level receiving m_i input blocks for compression, subscript i denoting a current level in the tree structure, whereby intermediate resulting numbers are produced, wherein said at least one first hash function additionally receives at least one cryptographic key as an input, and wherein different cryptographic keys are used in different levels of the tree structure, the method comprising processing an output of the tree-structure compression further to obtain said identification value,
characterized in that
- a residual data block is passed without compression from the current level to another, subsequent level in case n does not divide the number of input blocks m_i for said current level i, and in that
- data which represent a length L of the message are concatenated to the output to obtain a concatenated output, and/or to at least one of the intermediate resulting numbers.

2. A method according to claim 1, further comprising the step of inserting a set of predefined data at a predetermined position in the message, e.g. by appending the set of predefined data to the message, so that the length of the message with the appended set of data becomes a multiple of the length of the blocks.

3. A method according to claim 1 or 2, wherein the tree-structure compression is performed until the number of blocks is less than n.

4. A method according to claim 3, wherein said length L represents the length of the message without said appended set of data.
5. A method according to claim 4, wherein a hash function is applied to the concatenated output to obtain a compressed concatenated output, said hash function being one of:
- the at least one first hash function; and
- a second hash function.

6. A method according to any of the preceding claims, further comprising applying a further hash function to at least one of:
- said output,
- a further set of data derived from said output,
- said concatenated output, and
- said compressed concatenated output.

7. A method according to any of the preceding claims, further comprising applying a cryptographic function to said output or to a further set of data derived from said output.

8. A method according to claim 6 or 7, wherein at least one of:
- said second hash function; and
- said further hash function
makes use of at least one cryptographic key.

9. A method according to claim 8, wherein different cryptographic keys are used in one level of the tree structure.

10. A method according to claim 8, wherein the same cryptographic key is used in a single level of the tree structure.

11. A method according to any of the preceding claims, wherein at least one of:
- said first hash function;
- said second hash function; and
- said further hash function
is a universal hash function.

12. A method according to any of the preceding claims, wherein at least one of:
- said at least one first hash function;
- said second hash function; and
- said further hash function
comprises at least two different hash functions.

13. A method according to claim 12, wherein the at least two different hash functions compress different numbers n of blocks.

14. A method according to claim 12 or 13, wherein at least one of the at least two different hash functions compresses a variable number n of blocks.

15. A method according to any of claims 12-14, wherein the different hash functions use different cryptographic keys.

16. A method according to any of claims 8-15, comprising performing a plurality of tree-structure compressions of the message to obtain a plurality of results, and concatenating the plurality of results into a concatenated result.

17. A method according to claim 16, wherein different cryptographic keys are applied in the plurality of tree-structure compressions.

18. A method according to claim 16, wherein partly identical cryptographic keys are applied in the plurality of tree-structure compressions.

19. A computer system comprising a memory and a processor, the processor being programmed to carry out the method of any of claims 1-18.

20. A computer program product comprising means for performing the method of any of claims 1-18.

21. A method for generating an identification value for identifying an electronic message in a Message Authentication Code (MAC) function by application of at least one first hash function with fixed compression that compresses n blocks of data into a number of blocks which is smaller than n or into one single block, the hash function being repetitively applied in a tree-structure compression of the message, so that the message is being compressed in a plurality of tree-structure levels, each level receiving m_i input blocks for compression, subscript i denoting a current level in the tree structure, wherein said at least one first hash function additionally receives at least one cryptographic key as an input, and wherein different cryptographic keys are used in different levels of the tree structure, the method comprising processing an output of the tree-structure compression further to obtain said identification value,
characterized in that
the method comprises determining whether or not n divides the number of input blocks m_i for said current level i; and
if n does divide m_i: applying said at least one first hash function m_i/n times;
if n does not divide m_i:

- applying said at least one first hash function at most m_i/n times, whereby at least one residual data block is left unprocessed by the first hash function; and
- processing said at least one unprocessed data block by means of an auxiliary hash function which, in one single hash operation, compresses the at least one unprocessed data block into one single block, the auxiliary hash function having a compression rate, which is different from the compression rate of said first hash function.

22. A method according to claim 21, further comprising the step of inserting a set of predefined data at a predetermined position in the message, e.g. by appending the set of predefined data to the message, so that the length of the message with the appended set of data becomes a multiple of the length of the blocks.

23. A method according to claim 21 or 22, wherein the tree-structure compression is performed until the number of blocks is less than n.

24. A method according to claim 23, further comprising the step of concatenating the output with data which represent a length L of the message to obtain a concatenated output, the length L representing the length of the message without said appended set of data.

25. A method according to claim 24, wherein a hash function is applied to the concatenated output to obtain a compressed concatenated output, said hash function being one of:
- the at least one first hash function; and
- a second hash function.

26. A method according to any of claims 21-25, further comprising applying a further hash function to at least one of:
- said output,
- a further set of data derived from said output,
- said concatenated output, and
- said compressed concatenated output.

27. A method according to any of claims 21-26, further comprising applying a cryptographic function to said output or to a further set of data derived from said output.

28. A method according to any of claims 21-27, wherein at least one of:
- said at least one first hash function;
- said second hash function; and
- said further hash function
makes use of at least one cryptographic key.

29. A method according to claim 28, wherein different cryptographic keys are used in one level of the tree structure.

30. A method according to claim 28, wherein the same cryptographic key is used in a single level of the tree structure.

31. A method according to any of claims 21-30, wherein at least one of:
- said first hash function;
- said second hash function; and
- said further hash function
is a universal hash function.

32. A method according to any of claims 21-31, wherein at least one of:
- said at least one first hash function;
- said second hash function; and
- said further hash function
comprises at least two different hash functions.

33. A method according to claim 32, wherein the at least two different hash functions compress different numbers n of blocks.

34. A method according to claim 32 or 33, wherein at least one of the at least two different hash functions compresses a variable number n of blocks.

35. A method according to any of claims 32-34, wherein the different hash functions use different cryptographic keys.

36. A method according to any of claims 28-35, comprising performing a plurality of tree-structure compressions of the message to obtain a plurality of results, and concatenating the plurality of results into a concatenated result.

37. A method according to claim 36, wherein different cryptographic keys are applied in the plurality of tree-structure compressions.

38. A method according to claim 36, wherein partly identical cryptographic keys are applied in the plurality of tree-structure compressions.

39. A computer system comprising a memory and a processor, the processor being programmed to carry out the method of any of claims 21-38.

40. A computer program product comprising means for performing the method of any of claims 21-38.

41. A method for generating an identification value for identifying an electronic message, the method comprising the steps of:

- processing at least one block of a set of data derived from the message into a resulting number by means of a delta-universal hash function ; and
- computing a sum of the resulting number and a further block of data derived from the message to obtain a modified resulting number;
- using the modified resulting number further to obtain said identification value.

42. A method according to claim 41, wherein the hash function operates on a single block of data only.

43. A method according to claim 41 or 42, wherein the delta-universal hash function is repetitively applied in a tree-structure compression of the message, so that the message is being compressed in a plurality of tree-structure levels, each tree-structure receiving m_l input blocks for compression, the delta-universal hash function and the subsequent step of adding performing a compression of n data blocks into one single data block.

44. A method according to claim 43, wherein a residual data block is passed without processing thereof from a current level to another subsequent level in case n does not divide the number of input blocks m_i for said current level i.

45. A method according to any of claims 41-44, wherein the modified resulting number is determined by the function:
$(m_1+k \bmod 2^{32})\cdot(LSR(m_1,32)+LSR(k,32) \bmod 2^{32})+m_2 \bmod 2^{64}$,
where m_1 and m_2 denote two of said blocks of data, LSR(x,y) denotes a logical-shift-right by y bits of input x, and k denotes a cryptographic key, whereby m_1, m_2 and k are represented as 64 bit unsigned integers.

46. A computer system comprising a memory and a processor, the processor being programmed to carry out the method of any of claims 41-45.

47. A computer program product comprising means for performing the method of any of claims 41-45.